業務システムログの解析と活用によるシステムの改善 －お宝発見! ログ解析－

アブストラクト

１．本当のお宝は身近にある？（ログを有効活用していますか？）

「業務効率化の提言を求められたらどうしますか？ログを活用できますか？」

「トラブル対応に時間をとられていませんか？」

最近では、Ｊ－ＳＯＸや内部統制に代表されるコンプライアンス遵守の観点から、業務フローの明確化やシステムの証跡管理が必要となってきている。

また、ユーザ部門からは、業務効率化に向けた担当部門への提言や業務プロセスの最適化の指針、費用対効果といった情報の提供も求められる。

さらに、従来よりシステムを安定稼働させるためのトラブルの未然防止や、トラブル発生時のより迅速な対応も求められている。しかしながら、昨今のシステム複雑化傾向に伴い、システム管理者には多岐に渡る専門知識が必要とされており、知識の属人化、スキルを持った技術者不足による対応の不備等が問題となっている。

こういった要望に応えるために、対応や提言の基となる証跡－ログーの有効活用が以前にも増して重要視されてきている。

しかしながら、これまで各企業では多種のログを蓄積してきてはいたが、活用する機会もなく莫大な情報が無駄になっているケースが多くある。MOTTAINAI！

２．お宝へのアプローチ

どのようにしたら、目的もなく取り溜めていたログを有効活用できるのか？

従来のログは、主にスキルを持った人のトラブル対応にしか使われておらず、利用が不十分だった。この問題を解決するために､メーカーが設定した内容で出力されていたログをユーザの視点から見直し、どのようにすれば有効活用できるかを検討した。つまり、ゴミをお宝にする錬金術である。

ログは利用者の視点によって解釈が変わる。例えば、Web サーバのアクセスログをシステムの稼動確認で利用すればシステムログであり、業務分析で利用すれば業務ログとなる。

そこで、ログの種類を以下のとおり定義した(図表 1)。

図表１　ログの種類の定義

ログの種類	説明
業務ログ	業務分析で利用するログ。
システムログ	システムの障害や稼動状況を把握するのに利用するログ。

本分科会では、上記の 2 種類のログそれぞれに対して、以下のアプローチを試みた。

(1) バラバラになっている業務ログを集約化して新しい価値を見出す

(2) システムログを有効活用してシステムトラブル対応時の効率化を図る

３．お宝発見？！－業務ログ編

人の行動によりリスクが発生し、人の行動の結果、ログが出力される。つまり、ログはリスク、および、人の行動と密接に関連しているといえる。ログを解析することで、リスクヘッジや人の行動が可視化できると考え、実際に分科会メンバーの企業である A 社から入手したログ（Sendmail ログ、Web アクセスログ、入退室ログ、DHCP ログ）を使用し、リスクヘッジや人の行動に関する分析を行った。

結果として、単体のログでは把握することが困難なリスクや行動が、従業員マスタ、機器マスタおよびURL・業務・画面を結びつけるテーブルを作成し、ログを集約することによって、高い精度で把握できることが判明した。(図表 2)

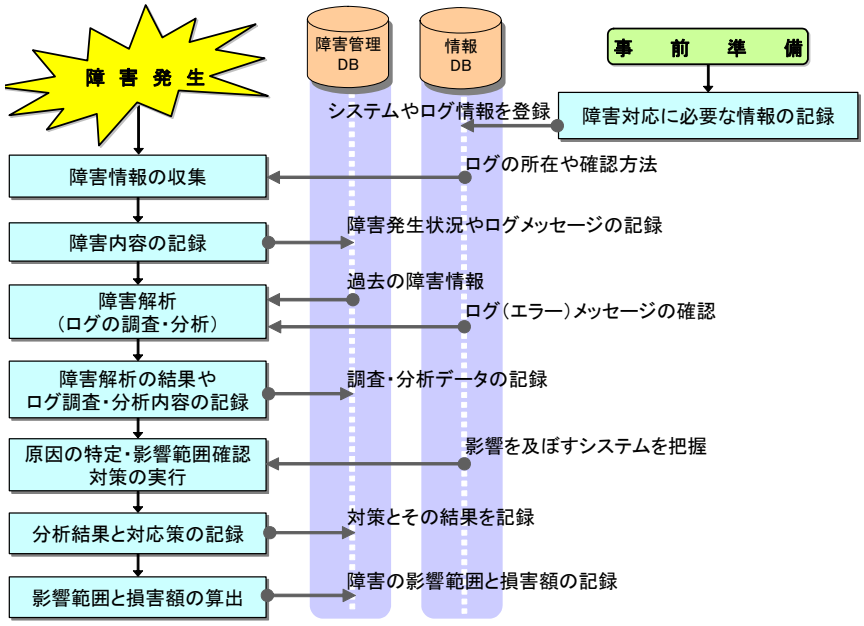
図表 2 人の一日

4．お宝発見？！ーシステムログ編

システムトラブル対応の効率化を図るために、各企業で現状のトラブル対応をどのように行っているか、障害解決プロセスを作成し、その内容から実際の現場でどのようなことが問題視されているか課題を導き出すことにした。

その結果､「障害が予防されない」､「障害解決に時間がかかる」の２つの問題点が明らかになった。このうち「障害を早期解決する」という点に着目し、理想の障害解決プロセスを策定した(図表 3)。

図表 3 障害解決プロセスのフロー



このプロセスは、過去事例を蓄積し知識ベースを構築する障害管理 DB と、企業の IT 資源情報を管理する情報 DB を用い､障害内容の記録が容易になり、過去事例をヒントにしたログの調査で障害原因の推定を支援するという特徴を持つ。

この障害解決プロセスが有効かを評価するため、このプロセスを体感できるデモアプリを構築し、本分科会メンバーの企業にモニタリングしていただき、アンケート結果をもとに評価した。

その結果、この障害解決プロセスを用いることにより、ログを活用して障害を素早く解決できると感じている人が多いことが明らかになり、本プロセスは有効であると言える。

5．まとめ

本分科会では、テーマを２つにわけ、研究、評価を行なった。それぞれで有用な結果を残し、今後のシステム管理、ひいては、システムを通した業務改善のサイクルの要として期待できる。

業務ログでは、目的もなく取り溜めていたゴミのようなログから、内部統制や業務改善につながる人の行動の見える化ができた。今後は、各社の様々なケースに対応できるような分析手法に関する研究を進めて欲しい。更に、自社開発のアプリケーションについても、本研究の統一フォーマットに準拠することで、分析の精度や幅を広げることが可能である。

システムログでは、トラブル解決の指針を決定することができた。これにより、属人的な作業を排除することへの道筋をつけることが可能となった。また、今回の研究を踏まえ、管理対象を拡張することで今後のシステム管理全般に対しての効率化が期待できる結果となった。

将来的には２テーマを統合することで、更に新たな発見ができるのではないかという思いもメンバー全員に残っている。

本研究成果を今後の業務の中で磨き、企業の発展、社会の発展のために尽力していきたい。